Password-Protected Secret Sharing Scheme

博士学位論文要約 (平成 27 年 3 月)

Password-Protected Secret Sharing Scheme
(パスワード付秘密分散共有方式)

Jun-ya Iwazaki (岩﨑 淳也)

1 Introduction

A file-hosting service enables us to easily store and access documents and data from mobile terminals as well as PC's, and to share them with others. Although the file-hosting service is so popular in the Internet community, we should note that there is a latent risk that we would lose the files we have stored.

In order to safely store some secret documents or data distributedly in several servers via insecure networks such as the Internet, Bagherzandi, Jarecki, Saxena and Lu proposed a password-protected secret sharing (PPSS, for short) scheme [1] in 2011. They proposed two PPSS protocols which achieve the following three properties: (**i**) both are secure against the corruption of the coalition of servers of size less than the specified threshold, which means that one can obtain no useful information about the password and the document even if some servers are corrupted, (**ii**) the user can be authenticated with a single password by all the servers, and (**iii**) there is no useful information about the password and the document in the interaction in a form that no polynomial time adversary can extract. In this thesis, we explore securer PPSS schemes, and propose some protocols.

We first consider security notions for PPSS schemes. Bagherzandi et al. focused on the interaction between the user and the servers, and formulated a security notion which we call the PPSS-security. A PPSS protocol is PPSS-secure if no polynomial time adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though he is allowed to adaptively interact with the servers and the user in impersonating manner. They proposed the protocol PPSS_2 which is PPSS-secure. In contrast, we focus on the process of generating a public parameter. Since the public parameter involves some information about the stored document in general, for any given public parameter, an adversary may obtain the stored document without corrupting the servers or impersonating the user. We propose another security notion for PPSS schemes with respect to the public parameter, named pparam-security. Intuitively, the pparam-security means that any public parameter does not contain any clue to the stored document in a way that an adversary could recognize. We show that PPSS_2 is not pparam-secure. We then give a protocol which is pparam-secure but not PPSS-secure. These results indicate that the pparam-security is independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa.

We next propose two PPSS protocols. One is ePPSS_2, an enhanced version of PPSS_2, where we prove that the protocol ePPSS_2 is both PPSS-secure and pparam-secure in the random oracle model. The other is a protocol named sPPSS which is both PPSS-secure and pparam-secure in the standard model. All the known protocols, including ePPSS_2, are provably secure in the random oracle model [1, 2, 3]. Hence, the protocol sPPSS is, to our best knowledge, the first protocol which is secure in the standard model.

2 Preliminaries

In this chapter, we describe notions and notations that are used through this thesis.

3 Security Notions for Password-Protected Secret Sharing Scheme

In this chapter, we focus on a public parameter which is generated by initialization algorithm on an input (p, d) of a password and a document, and we propose another PPSS security notion called the pparam-security. A pparam-attack game, for a PPSS scheme $\mathcal{P}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is as follows:

Initialization phase: $\mathcal{C}$ first executes the setup algorithm Setup on input 1^k, and gets a setup parameter λ. Then $\mathcal{C}$ sends λ to $\mathcal{A}$. $\mathcal{A}$ chooses two documents d_1 and d_2, and sends them to $\mathcal{C}$. $\mathcal{C}$ chooses $\beta \in_r \{1, 2\}$. Then $\mathcal{C}$ executes Init on an input (λ, p, d_β), and gets a pair $(\mathrm{pub}, \mathrm{sec})$, where $\mathrm{pub} = (\mathrm{pub}_1, \mathrm{pub}_2, \mathrm{pub}_3)$ is a public parameter and sec is a set of the secret seeds. Finally, $\mathcal{C}$ sends the public parameter pub to $\mathcal{A}$.

Attack phase: $\mathcal{A}$ is allowed to interact with $\mathcal{C}$. In each interaction, $\mathcal{A}$ sends any public parameters $\mathrm{pub}' = (\mathrm{pub}'_1, \mathrm{pub}'_2, \mathrm{pub}'_3)$ to $\mathcal{C}$. $\mathcal{C}$ plays the role in computing the "inverse" of Initialization procedure if $\mathrm{pub}_1 = \mathrm{pub}'_1$ and $\mathrm{pub}_3 \neq \mathrm{pub}'_3$. Then $\mathcal{C}$ returns a document d which satisfies $\mathsf{Init}(\lambda, p, d) = (\mathrm{pub}', \mathrm{sec}')$ for some password p and set sec' of secret seeds. Otherwise, $\mathcal{C}$ returns a special symbol $\perp$.

Challenge phase: $\mathcal{A}$ sends $\beta' \in \{1, 2\}$.

For $\beta = 1, 2$ and a security parameter k, let $P^{\beta}_{\text{pparam-atk}}(k)$ denote the probability that $\mathcal{A}$ sends 1 in Challenge phase of the pparam-attack game under the condition that $\mathcal{C}$ chooses β in Initialization phase, where the probability is taken over the random tapes of $\mathcal{A}$ and $\mathcal{C}$.

For a security parameter k and an adversary $\mathcal{A}$, we define $\mathrm{Adv}_{\mathcal{A}}(k)$ by

$$\mathrm{Adv}_{\mathcal{A}}(k) = \left| P^{1}_{\text{pparam-atk}}(k) - P^{2}_{\text{pparam-atk}}(k) \right|.$$

Definition 3.6 (pparam-security)**.** *A PPSS scheme $\mathcal{P}$ is (T, ϵ, q_A)-pparam-secure if for any security parameter k and any adversary $\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}(k) < \epsilon$ holds under the following conditions:*

1. *$\mathcal{A}$ is allowed to enter Attack phase at most q_A times, and*
2. *the running time of $\mathcal{A}$ is at most T.*

Intuitively, a PPSS protocol is pparam-secure if no polynomial time adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though he is allowed to adaptively receive sample pairs of the public parameter and the stored document.

We show that the protocol PPSS_2 [1] is not pparam-secure.

Proposition 3.8. *For the protocol PPSS_2, there exists a PPT adversary $\mathcal{A}$ such that $\mathrm{Adv}_{\mathcal{A}}(k) = 1$, that is, the protocol PPSS_2 is not $(T, 1, 1)$-pparam-secure.*

We next reveal the relationship between the pparam-security and the PPSS-security. We propose a protocol named Protocol 3.2 in this thesis, and show that the protocol is pparam-secure but not PPSS-secure.

Let $Q = 2q + 1$ be a safe prime, and let $\mathbb{G}_q$ be the subgroup of $\mathbb{Z}_q^*$ of order q. Choose a generator g of $\mathbb{G}_q$. Then we define the language $\mathcal{L}_E^{\mathrm{pub}}$ as follows [4]:

$$\mathcal{L}_E^{\mathrm{pub}} = \left\{ (u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d}) \in \mathbb{G}_q^4 \mid \exists (r_{1,d}, r_{2,d}) \in \mathbb{Z}_q^2 \text{ s.t. } u_{1,d} = g^{r_{1,d}}, u_{2,d} = g^{r_{2,d}}, v_{1,d}/v_{2,d} = y_1^{r_{1,d}}/y_2^{r_{2,d}} \right\},$$

where $y_1 = g^{x_1}$ and $y_2 = g^{x_2}$ for some $x_1, x_2 \in \mathbb{Z}_q$.

Proposition 3.9. *Assume that the following properties hold:*

- *the protocol PPSS_2 is $(T, \epsilon, 0)$-pparam-secure, and*
- *the proof system $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ used in Protocol 3.2 is $(T_S, 1, q_H^S, \epsilon_{\mathrm{ZK}}, \epsilon_{\mathrm{SS}})$-SS-NIZK.*

Then Protocol 3.2 is (T', ϵ', q_A)*-pparam-secure, where* $T' \leq T - T_S - q_A f_A$, $q_A \leq q_H^S$ and $\epsilon' \leq 2\epsilon + 6\epsilon_{\mathrm{SS}}$ *for some polynomial* f_A *in* n, t *and* k.

Proposition 3.10. *Protocol 3.2 is not PPSS-secure.*

Propositions 3.9 and 3.10 indicate that the pparam-security is independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa.

We then improve the protocol PPSS_2 by using the twin-encryption version of the ElGamal encryption scheme [4], and show that the improved protocol ePPSS_2 is pparam-secure.

Theorem 3.11. *Assume that the following properties hold:*

- *the protocol* PPSS_2 *is* $(T, \epsilon, 0)$*-pparam-secure, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *used in the protocol* ePPSS_2 *is* $(T_S, 1, q_H^S, \epsilon_{\mathrm{ZK}}, \epsilon_{\mathrm{SS}})$*-SS-NIZK.*

Then the protocol ePPSS_2 *is* (T', ϵ', q_A)*-pparam-secure, where* $T' \leq T - T_S - q_A f_A$, $q_A \leq q_H^S$ and $\epsilon' \leq 2\epsilon + 6\epsilon_{\mathrm{SS}}$ *for some polynomial* f_A *in* n, t *and* k.

Theorem 3.12. *Assume that the following properties hold:*

- *the* DDH *problem is* $(T_{\mathrm{ddh}}, \epsilon_{\mathrm{ddh}})$*-hard,*
- *the proof systems* $(\mathcal{P}(\mathcal{L}_{S1}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{S1}^{\mathrm{pub}}))$, $(\mathcal{P}(\mathcal{L}_U^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_U^{\mathrm{pub}}))$ *and* $(\mathcal{P}(\mathcal{L}_{S2}^{\mathrm{pub},j}), \mathcal{V}(\mathcal{L}_{S2}^{\mathrm{pub},j}))$ *used in the protocol* PPSS_2 *are* $(T_S, q_P^S, q_H^S, \epsilon_{\mathrm{SS}}, \epsilon_{\mathrm{ZK}})$*-SS-NIZK, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *is* $(T_S, 1, q_H^S, \epsilon_{\mathrm{SS}}, \epsilon_{\mathrm{ZK}})$*-SS-NIZK.*

Then the protocol ePPSS_2 *is* $(n, t, q_U, q_S, T, \epsilon)$*-PPSS-secure, where*

$$\max\{nq_U, q_S\} \leq q_P^S, q_H^S,\ T \leq T_{\mathrm{ddh}} - 4T_S - q_U f^U - q_S f^S - f^I$$

for some polynomials f^U, f^S *and* f^I *in* n, t *and* k*, and*

$$\epsilon \leq 8\epsilon_{\mathrm{ZK}} + (4nq_Uq_S + 6nq_U - 4nq_S + 6q_S)\epsilon_{\mathrm{SS}} + (2q_Uq_S + 3q_U + 2q_S + 7)\epsilon_{\mathrm{ddh}} + \frac{36q_Uq_S(q-1)}{q^2} + \frac{8q_U(4q^2 - 5q + 2)}{q^3} + \frac{q_S(13q^3 - 32q^2 + 42q - 16)}{q^4} + \frac{3}{q}.$$

4 Password-Protected Secret Sharing Scheme without Random Oracles

In this chapter, we propose a PPSS scheme sPPSS, and show that the protocol is PPSS-secure and pparam-secure in the standard model.

Let $\mathbb{G}_N$ be a cyclic group of order $N = q_1q_2$ for some primes q_1 and q_2, and let $\mathbb{G}_{q_1}$ be the subgroup of $\mathbb{G}_N$ of order q_1. Choose generators g and g_1 of $\mathbb{G}_N$ and $\mathbb{G}_{q_1}$, respectively, and set $y_1 = g_1^{x_1}$, $y_2 = g_1^{x_2}$ and $y = g_1^{x_1x_2}$ for some $x_1, x_2 \in \mathbb{Z}_N$. Then we define the languages $\mathcal{L}_{S1}^{\mathrm{pub}}$, $\mathcal{L}_U^{\mathrm{pub}}$ and $\mathcal{L}_{S2}^{\mathrm{pub},j}$ as follows:

$$\mathcal{L}_{S1}^{\mathrm{pub}} = \{(a_{1,j}, a_{2,j}, b_{1,j}, b_{2,j}) \in \mathbb{G}_N^4 \mid \exists t_j \in \mathbb{Z}_N \text{s.t. } (a_{1,j}, a_{2,j}, b_{1,j}, b_{2,j}) = (y_1^{t_j}, y_2^{t_j}, u_{1,p}^{t_j}, u_{2,p}^{t_j})\},$$

$$\mathcal{L}_U^{\mathrm{pub}} = \big\{(a_{1,j}, a_{2,j}, e_{1,j}, e_{2,j}, u_{1,\tilde{p}}, u_{2,\tilde{p}}, v_{\tilde{p}}, \hat{u}_{1,\tilde{p}}, \hat{u}_{2,\tilde{p}}, \hat{v}_{\tilde{p}}) \in \mathbb{G}_N^{10} \mid \exists (r_{1,\tilde{p}}, r_{2,\tilde{p}}, \tilde{p}, \hat{r}_{1,\tilde{p}}, \hat{r}_{2,\tilde{p}}) \in \mathbb{Z}_N^5$$
$$\text{s.t. } (e_{1,j}, e_{2,j}, u_{1,\tilde{p}}, u_{2,\tilde{p}}, v_{\tilde{p}}, \hat{u}_{1,\tilde{p}}, \hat{u}_{2,\tilde{p}}, \hat{v}_{\tilde{p}}) = (a_{1,j}^{r_{1,\tilde{p}}}, a_{2,j}^{r_{2,\tilde{p}}}, y_1^{r_{1,\tilde{p}}}, y_2^{r_{2,\tilde{p}}}, y^{r_{1,\tilde{p}}+r_{2,\tilde{p}}}g^{\tilde{p}}, \hat{y}_1^{\hat{r}_{1,\tilde{p}}}, \hat{y}_2^{\hat{r}_{2,\tilde{p}}}, \hat{y}^{\hat{r}_{1,\tilde{p}}+\hat{r}_{2,\tilde{p}}}\hat{g}^{\tilde{p}})\big\},$$

and

$$\mathcal{L}_{S2}^{\mathrm{pub},j} = \Big\{(u_{1,z_j}, u_{2,z_j}, v_{z_j}, a_{1,j}, a_{2,j}, v_p/v_{\tilde{p}}, (u_du_2)^{\lambda_j}, u_1^{\lambda_j}) \in \mathbb{G}_N^8 \mid$$
$$\exists (s_1, s_2, x_{1,j}, x_{2,j}, t_j, r_{1,j}, r_{2,j}) \in \mathbb{Z}_N^7 \text{ s.t. } (y_{1,j}, y_{2,j}, a_{1,j}, a_{2,j}, u_{1,z_j}, u_{2,z_j}, v_{z_j})$$
$$= (g_1^{x_{1,j}}, g_1^{x_{2,j}}, y_1^{t_j}, y_2^{t_j}, \bar{y}_1^{r_{1,z_j}}, \bar{y}_2^{r_{2,z_j}}, u_{1,z_j}^{s_2}u_{2,z_j}^{s_1}(v_p/v_{\tilde{p}})^{t_j}(u_du_2)^{\lambda_j x_{1,j}}u_1^{\lambda_j x_{2,j}})\Big\},$$

where $u_{1,p}, u_{2,p}, \hat{y}_1, \hat{y}_2, \bar{y}_1, \bar{y}_2 \in \mathbb{G}_{q_1}$.

Theorem 4.3. *The encryption scheme of Libert and Yung [5] is (T, ϵ, q_A)-IND-CCA secure, then the protocol* sPPSS *is (T', ϵ, q_A)-pparam-secure, where $T' \leq T - q_A f_A$ for some polynomial f_A in n, t and k.*

Theorem 4.4. *Assume that the following properties hold:*

- *the DLIN problem is $(T_{\mathrm{DLIN}}, \epsilon_{\mathrm{DLIN}})$-hard,*
- *the SD problem is $(T_{\mathrm{SD}}, \epsilon_{\mathrm{SD}})$-hard,*
- *the proof systems $(\mathcal{P}(\mathcal{L}_{S1}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{S1}^{\mathrm{pub}}))$, $(\mathcal{P}(\mathcal{L}_{U}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{U}^{\mathrm{pub}}))$ and $(\mathcal{P}(\mathcal{L}_{S2}^{\mathrm{pub},j}), \mathcal{V}(\mathcal{L}_{S2}^{\mathrm{pub},j}))$ used in the protocol* sPPSS *are $(T_S, q_P^S, \epsilon_{\mathrm{SS}}, \epsilon_{\mathrm{ZK}})$-SS-NIZK, and*
- *a signature scheme Σ chosen in Step 5 of* Setup *of the protocol* sPPSS *is a one-time signature.*

Then the protocol sPPSS *is $(n, t, q_U, q_S, T, \epsilon)$-PPSS-secure, where*

$$\max\{nq_U, q_S\} \leq q_P^S,\ T \leq \max\{T_{\mathrm{SD}}, T_{\mathrm{DLIN}}\} - 3T_S - q_U f^U - q_S f^S - f^I,$$

for some polynomials f^U, f^S and f^I in n, t and k, and

$$\epsilon \leq 6\epsilon_{\mathrm{ZK}} + 9\epsilon_{\mathrm{SD}} + (2n(q_U - 1)q_S + 2q_U + 1)\epsilon_{\mathrm{DLIN}} + 2n((q_U - 1)q_S + 2q_U)\epsilon_{\mathrm{SS}} + \omega(k),$$

where ω is negligible in k.

5 Conclusion

In this thesis, we have explored securer PPSS schemes, and proposed some protocols.

In Chapter 3, we have investigated security notions for PPSS schemes. First, we first have proposed another security notion for PPSS schemes, named pparam-security. The pparam-security intuitively means that any public parameter does not include any clue to the stored document in a way that an adversary could recognize. We have shown that the protocol PPSS_2 proposed in [1] is not pparam-secure. We then have given a protocol which is pparam-secure but not PPSS-secure. These results indicate that the pparam-security is logically independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa. Finally we have proposed the enhanced protocol ePPSS_2, and shown that ePPSS_2 is pparam-secure and PPSS-secure. This protocol is the first protocol which is both PPSS-secure and pparam-secure.

In Chapter 4, we have proposed the protocol sPPSS which is both pparam-secure and PPSS-secure in the standard model. All the known PPSS protocols, including ePPSS_2, are provably secure in the random oracle model. The protocol sPPSS is, to our best knowledge, the first PPSS protocol which is secure in the standard model.

References

[1] A. Bagherzandi, S. Jarecki, N. Saxena and Y. Lu, "Password-Protected Secret Sharing," Proc. CCS'11, pp.433-444, 2011.

[2] J. Camenisch, A. Lysyanskaya and G. Neven, "Practical Yet Universally Composable Two-Server Password-Authenticated Secret Sharing," Proc. CCS'12, pp.525–536, 2012.

[3] J. Camenisch, A. Lehmann, A. Lysyanskaya and G. Neven, "Memento: How to Reconstruct Your Secrets from a Single Password in a Hostile Environment," CRYPTO'14, LNCS, vol.8617, pp.256-275, Springer, 2014.

[4] P. A. Fouque and D. Pointcheval, "Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks," ASIACRYPT'01, LNCS, vol.2248, pp.351-368, Springer, 2001.

[5] B. Libert and M. Yung, "Non-interactive CCA-secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions," TCC'12, LNCS, vol.7194, pp.75–93, 2012.